The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

Computrition Hospitality Suite (Computrition)
Enterprise Program Management Office (EPMO)

Date PIA submitted for review:
14 July 2020

System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewel@va.gov">Rita.Grewel@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Karen McQuaid</td>
<td><a href="mailto:Karen.McQuaid@va.gov">Karen.McQuaid@va.gov</a></td>
<td>708-483-5311</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Christopher Brown</td>
<td><a href="mailto:Christopher.Brown1@va.gov">Christopher.Brown1@va.gov</a></td>
<td>202-270-1432</td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

Computrition is a software package designed to facilitate food service in health institutions through various integrated modules for inventory management, menu management, meal planning, diet management while providing enhanced functionality to patients with a variety of room service options. Computrition integrates with most major electronic health record and manage systems utilizing industry standard interfaces, while also providing an interface to allow 3rd party Commercial Off The Shelf (COTS) products used by the VA as listed in table 4.1 to access and utilize specific Computrition functionality to incorporate additional functionality.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• **NIST 800-144** states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

• **What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally?** Would the reputation of the CSP or its customers (VA) be affected?

Computation is used in over 130 Veteran Health Agency (VHA) facilities in Nutrition and Food Service (NFS) and managed under the auspice of Enterprise Program Management Office (EPMO). Computation is a Citrix-based application that is incorporated as part of the GSS for former regions 1, 2, 3 and 4. Computation and its modules have been vetted through TRM (Technical Review Model) processes. The completion of this PIA will not result in any business or technology changes. Computation does not utilize Cloud technology. The number of individuals with information stored would vary by facility. Computation will store Personally Identifiable Information (PII)/Protected Health Information (PHI) for inpatient veterans whose information is received from the Department of Veteran Affairs (VA) Electronic Health Record (EHR) systems, throughout this document EHR represents VistA. Only patient information stored are those actively admitted as inpatient. Computation has several modules utilized by VHA sites across the country:

• **Food Operations Manager (FOM):** Computation offers a wide array of enterprise-level software features and services that help efficiently plan, organize, and manage production, inventory, and ordering operations. Computation delivers superior management functionality and reporting options, gives access to valuable information that is virtually impossible to collect in a non-automated environment.

• **Cost savings/Reduced waste:** Store a history of post meal counts to assist in forecasting future production and order amounts; scale recipe and menu amounts according to production needs. Improved nutrition quality for Veterans: Analyze nutrient information at the food item, recipe, and menu level; ability to populate nutrition labels for patient education and display in cafeterias. Staff workflow efficiencies: Implement order entry interfaces with major vendors; Update vendor item prices automatically that reflect costs at the food item, recipe, and menu level; Merge information from a master set of data out to site; save reports in a variety of Windows formats.

• **Nutrition Care Management (NCM):** streamlines workflow with the automation of manual processes. Administering an electronic patient cardex and better managing tray tickets and diet orders are just a few fundamental improvements. Having preventative food safety measures in place is vital in eliminating the risk of errors, harmful reactions or even fatal outcomes related to food allergies. NCM equips nutrition services to practice patient safety with features that can trigger alerts, customize tray tickets and modify menus to guarantee the food served coincides with the patient’s existing diet order. All patient information is securely transmitted across the one-way interface between VA EHR and Computation. Improved safety/quality of Veteran nutrition care: Menu correction for food/drug interactions; Track diet order history; Ensure that patients are never served food that they dislike, are allergic to or that are inappropriate for their diet order; improved patient satisfaction scores. Staff workflow efficiencies: Redirect staff resources due to elimination of manual processes; ability to populate detailed reports to improve nutritional quality, safety and variety of menu items.

• **Bedside Connect:** Bedside Connect is an add-on module takes advantage of a tablet with touch screen abilities so that the bedside meal selection experience is easy and efficient for the user and quick and pleasant for the patient. Improved safety/quality of Veteran nutrition...
care: Increases patient-staff interaction, helping to boost satisfaction scores; Take bedside patron meal orders using a tablet, Nutrition information is available to give patients feedback on their meal selections and can aide as a teaching tool for encouraging healthy meal choices. Staff workflow efficiencies: Significantly expedites the meal selection process; Flags selections for likes, dislikes, and allergies with the ability to enter them on the spot; find out who hasn’t ordered their meal(s) yet, ensuring that your staff visit those patients and gather their selections.

- Touch Point Dining: This add-on module will allow patients to order meals on their TV via the GetWellNetwork or other TV systems on the patients preferred schedule not dependent on any staff being in the room.
- Improved safety/quality of Veteran nutrition care: improves patient satisfaction scores; Nutrition information is available to give patients feedback on their meal selections and can aide as a teaching tool for encouraging healthy meal choices; Menus specific for patients with allergies and restricted food items removed, ensuring that menu offerings are appropriate for their therapeutic diets. Staff workflow efficiencies: Reduce the number of patients needing staff to visit to order meals.
- Cost savings/Reduced waste: Diminish food waste by delivering food that patients request; Increase labor savings by decreasing diet office staff required to operate a room service call center; Reduce the cost of and reliance on paper menus
- Room Service: Room service is an add-on module based on the hotel model, patients can similarly place an order from their room by selecting items from a restaurant-style menu, typically delivered within 45 minutes of ordering. Patient can order what they want (within diet restrictions), how they want it, when they want it. Improved safety/quality of Veteran nutrition care: flexibility in meal service, increasing patient satisfaction, improved food intakes and nutritional status due to Veterans being served the foods they prefer; Nutritional analysis includes patient meal intake calculations. Cost savings/Reduced waste: less food waste since the Veteran receive the foods they want/like versus items that are part of a standard menu that may not meet their preferences.
- Tray in Motion: Tray in Motion is an add-on module that is a real-time, integrated application enabling staff to efficiently manage tray delivery and retrieval of patient meals. A tool that utilizes barcode scanners with numerous benefits, Tray In Motion promotes patient safety by ensuring that the right meals are delivered in a timely manner to specific patients. It acts as a safeguard against delivery of an incorrect therapeutic diet and enables Nutrition Services teams to track and benchmark their individual and shift delivery times. Improved safety/quality of Veteran nutrition care: Acts as a safeguard against delivery of an incorrect therapeutic diet, increased patient satisfaction. Staff workflow efficiencies: Provides immediate tray delivery information to diet office staff and improves the meal delivery process flow and exposes areas that delay the tray transit time.
- The legal authority to operate Computrition falls under Executive Order 9397 and 32 CFR 505.4(a)(b)
- The following VA System of Record Notices (SORNs) which are published in the Federal Register and available online:
  - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10P2 (Oct. 31, 2012, as amended)
  - National Patient Database-VA, SORN 121VA19 (May 11, 2012, as amended)
  
  https://www.oprm.va.gov/docs/CurrentSORNList_4_29_20.pdf
Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy-Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

- Admission date
- Diet orders from Electronic Health Record
- Allergies

PII Mapping of Components

Computrition Hospitality Suite has 5 database that stores patient data. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Computrition Hospitality Suite and the reasons for the collection of the PII are in the table below.
## PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCR HS</td>
<td>No</td>
<td>Yes</td>
<td>Patient, SSN, DOB, room #/location, diet/formula order, allergies, MRN</td>
<td>Identify patient, ensure meals are delivered to the correct location and patient. Ensure patients are not fed foods they are allergic to.</td>
<td>Database servers are encrypted and fully compliant with VA Database baseline standards.</td>
</tr>
<tr>
<td>DVR HS</td>
<td>No</td>
<td>Yes</td>
<td>Patient, SSN, DOB, room #/location, diet/formula order, allergies, MRN</td>
<td>Identify patient, ensure meals are delivered to the correct location and patient. Ensure patients are not fed foods they are allergic to.</td>
<td>Database servers are encrypted and fully compliant with VA Database baseline standards.</td>
</tr>
<tr>
<td>LIT HS</td>
<td>No</td>
<td>Yes</td>
<td>Patient, SSN, DOB, room #/location, diet/formula order, allergies, MRN</td>
<td>Identify patient, ensure meals are delivered to the correct location and patient. Ensure patients are not fed foods they are allergic to.</td>
<td>Database servers are encrypted and fully compliant with VA Database baseline standards.</td>
</tr>
<tr>
<td>ORL HS</td>
<td>No</td>
<td>Yes</td>
<td>Patient, SSN, DOB, room</td>
<td>Identify patient, ensure meals</td>
<td>Database servers are encrypted and fully compliant</td>
</tr>
</tbody>
</table>
VFH

1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VA EHR is the source of information for Computrition. The information in Computrition is pushed from the VA EHR to Computrition via a unidirectional Health Level 7 (HL7) interface. Updates to information must be made in the VA EHR and pushed to Computrition via the same unidirectional HL7 interface.
1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number. This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

All information is provided by the Electronic Health Record via HL7 interface to Computrition and verified during patient contact.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

The PII collected ensures HL7 messages, such as allergies, diet orders, room location, and special services, are transmitted to the correct patient food service record. It also ensures that meals are delivered to the correct location and patient, allowing for food service workers to Positive Patient Identification when delivering meals.

1.5 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Sites are encouraged to check accuracy of all information that comes across the interface. Sites have been encouraged to compare diet orders in Computrition to VA EHRM for discrepancies. Computrition information is used in conjunction with existing data from VA EHRM. The information collected is a combination of Personal Identifiable Information (PII) and Protected Health Information (PHI).

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

This question is related to privacy control AP-1, Authority to Collect

SSN serves as the Medical Record Number and Unique Identifier for the Veteran and is collected by the VA EHR which then pushes the information to Computrition. The legal authority is Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual’s rights, benefits, and privileges under federal programs. Also to include Title 38, United States Code, Sections 501(b) and 304; and Title 38, United States Code, section 7301(a).

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
Follow the format below when entering your risk assessment:

**Privacy Risk:** The Computrition software suite collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

**Mitigation:** Veterans Health Administration (VHA) deploys extensive security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

**Section 2. Uses of the Information**

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 **Describe how the information in the system will be used in support of the program’s business purpose.**

*Identify and list each use (both internal and external to VA) of the information collected or maintained.*

*This question is related to privacy control AP-2, Purpose Specification.*

- **Name:** Used to identify the patient and verify diet orders, allergies and in other forms of communication
- **Social Security Number:** Used as a patient identifier
- **Date of Birth:** Used to identify age and confirm patient identity
- **Medical Record Number:** Used as a patient identifier in Computrition
- **Admission Date:** To notify the kitchen of a new admission and need for a tray
- **Diet Order from CPRS:** The kitchen needs to know what the patient’s diet order is to ensure safe meal delivery to patient
- **Allergies:** Ensure patients are not fed food they are allergic to

2.2 **What types of tools are used to analyze data and what type of data may be produced?**
Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual’s existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Computrition does not analyze patient data.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Each NFS service has system administrators who maintain access to Computrition and ensures safeguards of PII/PHI. It is the responsibility of NFS to ensure that employees who have Computrition access within the service stay current on required HIPPA and Privacy training, otherwise access to the computers are removed.

Access to Computrition is controlled at the local site level using approval processes defined by the local site Nutrition and Food Services (NFS) department. Inside of Computrition, each site works with the vendor to build a customized series of “security levels” that allows them to build multiple levels of authorization appropriate to the data access requirements of individual jobs. Each
Computrition user is authorized by the appropriate supervisor at their local site and is granted access to Computrition and is assigned to the security level deemed appropriate to fulfill their job duties.

The vendor does not have direct access to any Computrition data, however they may see PHI/PII while performing helpdesk support functions for end users or technical staff. A Business Associate Agreement is in place to cover any PHI/PII that is seen during these helpdesk sessions.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

The information listed in Section 1.1 is retained in the Computrition database and is deleted 90 days after patient discharge unless the local facility chooses to retain for a longer period. Information retained is name, date of birth, SSN, allergies, MRN.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. This question is related to privacy control DM-2, Data Retention and Disposal.

The information listed in Section 1.1 is retained in the Computrition database and is deleted based upon the Records Control Schedule (RCS).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule.
The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. This question is related to privacy control DM-2, Data Retention and Disposal.

The data retention period has been approved by NARA and is processed according to the following:
- National Archives and Records Administration: [www.nara.gov](http://www.nara.gov)

According to Records Control Schedule 10-1, (See page 251 and 252 of RCS 10-1) the information is considered Temporary and the disposition depends on information in Computrition.

### 3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal.

An automated process runs each day to remove information that meet or exceed retention timeframe criteria. Data contained in Computrition can be manually removed if necessary, based upon the disposition in RCS 10-1.

### 3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Computrition does not use PII for research, testing, or training.

### 3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of
PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

**Principle of Minimization:** Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:** The risk to maintaining data within the Computrition system is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached

**Mitigation:** All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness & Rules of Behavior training annually. Computrition adheres to all information security requirements instituted by the VA Office of Information and Technology (OI&T). RCS 10-1 is being followed, as approved by NARA

**Section 4. Internal Sharing/Receiving/Transmitting and Disclosure**

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

**Data Shared with Internal Organizations**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
</table>
| Vista | To enable authorized personnel to view Veteran’s Patient information in a timely manner. | PII-PHI as identified in section 1.1  
• Name  
• Social Security Number  
• Date of Birth  
• Medical Record Number  
• Other Unique Identifying Number  
• Admission date  
• Diet orders from Electronic Health Record  
• Allergies | Unidirectional HL7 interface from Vista to Comptrition |

GetwellNetwork (GWN)  
To allow patients to order room service from their television.  
PII-PHI as identified in section 1.1  
• Name  
• Social Security Number  
• Date of Birth  
• Medical Record Number  
• Other Unique Identifying Number |

### 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.  
This question is related to privacy control UL-1, Internal Use.
Follow the format below:

**Privacy Risk:** There is a risk that information may be shared with unauthorized VA programs or systems or that data could be shared inappropriately.

**Mitigation:** Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

## Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

**Note:** This question is #7 in the Privacy Threshold Analysis.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties
### Data Shared with External Organizations

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Not applicable.

**5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

**Privacy Risk:** no risk as system does not share information outside of the Department.

**Mitigation:** N/A

### Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

**6.1 Was notice provided to the individual before collection of the information?** If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a
Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The following VA System of Record Notices (SORNs) which are published in the Federal Register and available online:

- Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10P2 (Oct. 31, 2012, as amended)
- National Patient Database-VA, SORN 121VA19 (May 11, 2012, as amended)

https://www.oprm.va.gov/docs/CurrentSORNList_4_29_20.pdf

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent
Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Risk: There is a risk that veterans and other members of the public will not know that the Computrition Hospital Suite exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR. The SORNs listed in 6.1 are also a form of notice, as well as this PIA.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).
If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Computrition receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR.
7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:

**Principle of Individual Participation:** Is the individual provided with the ability to find out whether a project maintains a record relating to him?

**Principle of Individual Participation:** If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

**Principle of Individual Participation:** Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

**Risk:** There is a risk that individuals are unaware of how to access or correct their information in the system.

**Mitigation:** Comptrution receives all data from VA EHR and this would be covered in the applicable PIA for the designated EHR. Information in the system is only collected from other systems. Access, redress, and correction procedures are provided by the source systems and are in their PIAs.

---

**Section 8. Technical Access and Security**

The following questions are intended to describe technical safeguards and security measures.

**8.1 What procedures are in place to determine which users may access the system, and are they documented?**

*Describe the process by which an individual receives access to the system.*

*Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

*Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.
Access is requested per Department of Veteran Affairs and local VAMC policies utilizing Electronic Computer Access Requests (ECAR) or by other individual local processes. System administrators submit access requests based on need to know and job duties. These requests are submitted for VA employees, and contractors. They are processed through the appropriate approval processes. NFS Supervisors assign security levels/permissions to allow individual users read only or read/write access to the information as appropriate.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Comptrition and the VA ensure that all personnel including contractors who have access to VA computers must complete the onboarding and annual Privacy and Information Security Awareness mandatory training.

Contracts are reviewed by the appropriate contract authority i.e., Contracting Officer Representative (COR), Contracting Officer (CO), Contract Review Committee. Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VA HIPAA Privacy Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question.

In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.
All VA employees who have access to VA computers must complete the onboarding and annual mandatory Privacy and Information Security Awareness Training. In addition, all employees who interact with patient sensitive medical information must complete the mandated VHA HIPAA Privacy Training. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject-specific training on an as needed basis.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

If No or In Process, provide your Initial Operating Capability (IOC) date.

No, the IOC date is October 24, 2020.
## Section 9. References

### Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td><strong>Authority and Purpose</strong></td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td><strong>Accountability, Audit, and Risk Management</strong></td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td><strong>Data Quality and Integrity</strong></td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td><strong>Data Minimization and Retention</strong></td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td><strong>Individual Participation and Redress</strong></td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td><strong>Use Limitation</strong></td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

RITA K GREWAL
114938
Digitally signed by RITA K GREWAL 114938
Date: 2020.09.17 06:22:13 -04'00'

Privacy Officer, Rita Grewal

Karen A. McQuaid 321576
Digitally signed by Karen A. McQuaid 321576
Date: 2020.09.16 14:54:25 -05'00'

Information Security Systems Officer, Karen McQuaid

Christopher Brown 101386
Digitally signed by Christopher Brown 101386
Date: 2020.09.22 11:48:55 -05'00'

Information System Owner, Christopher Brown
APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).